

On the class of diffusion operators for fast quantum search

Avatar Tulsi

Department of Physics, IIT Bombay, Mumbai-400076, India*

Grover's quantum search algorithm evolves a quantum system from a known source state $|s\rangle$ to an unknown target state $|t\rangle$ using the selective phase inversions, I_s and I_t , of these two states. In one of the generalizations of Grover's algorithm, I_s is replaced by a general diffusion operator D_s having $|s\rangle$ as an eigenstate and I_t is replaced by a general selective phase rotation I_t^ϕ . A fast quantum search is possible as long as the operator D_s and the angle ϕ satisfies certain conditions. These conditions are very restrictive in nature. Specifically, suppose $|\ell\rangle$ denote the eigenstates of D_s corresponding to the eigenphases θ_ℓ . Then the sum of the terms $|\langle\ell|t\rangle|^2 \cot(\theta_\ell/2)$ over all $\ell \neq s$ has to be almost equal to $\cot(\phi/2)$ for a fast quantum search. In this paper, we show that this condition can be significantly relaxed by introducing appropriate modifications of the algorithm. This allows access to a more general class of diffusion operators for fast quantum search.

PACS numbers: 03.67.Ac

I. INTRODUCTION

Grover's quantum search algorithm or more generally quantum amplitude amplification evolves a quantum system from a known *source* state $|s\rangle$ to an unknown but desired *target* state $|t\rangle$ [1–3]. It does so by using selective phase inversion operators, I_s and I_t , of these two quantum states. The algorithm iteratively applies the operator $\mathcal{A}(s, t) = -I_s I_t$ on $|s\rangle$ to get $|t\rangle$. The required number of iterations is $O(1/\alpha)$ where $\alpha = |\langle t|s\rangle|$. For search problem, $|s\rangle$ is chosen to be the uniform superposition of all N basis states to be searched i.e. $|s\rangle = \sum_i |i\rangle/\sqrt{N}$. In case of a unique solution, the target state $|t\rangle$ is a unique basis state and $\alpha = |\langle t|s\rangle| = 1/\sqrt{N}$. Thus Grover's algorithm outputs a solution in just $O(\sqrt{N})$ time steps whereas *classical* search algorithms take $O(N)$ time steps to do so. Quantum search algorithm and amplitude amplification are proved to be strictly optimal [4].

A generalization of quantum search algorithm was presented in [5]. The general quantum search algorithm (hereafter referred to as general algorithm) replaces I_s by a more general diffusion operator D_s with the only restriction of having $|s\rangle$ as an eigenstate. This restriction is reasonable as the diffusion operator should have some special connection with the source state. Let the normalized eigenspectrum of D_s be given by $D_s|\ell\rangle = e^{i\theta_\ell}|\ell\rangle$ with $|\ell\rangle$ as the eigenstates and $e^{i\theta_\ell}$ (θ_ℓ) as the corresponding eigenvalues (eigenphases). We choose $D_s|s\rangle = |s\rangle$, i.e. $\theta_{\ell=s} = 0$. The general algorithm also replaces I_t by a general selective phase rotation I_t^ϕ which multiplies $|t\rangle$ by a phase factor of $e^{i\phi}$ but leaves all states orthogonal to $|t\rangle$ unchanged. When ϕ is π , I_t^ϕ becomes I_t . Thus the general algorithm iterates the operator $\mathcal{S} = D_s I_t^\phi$ on $|s\rangle$ and its dynamics can be understood by analyzing the eigenspectrum of \mathcal{S} .

This analysis was done in [5] and we found that the

performance of the general algorithm depends upon the moments Λ_1 and Λ_2 given by

$$\Lambda_p = \sum_{\ell \neq s} |\langle\ell|t\rangle|^2 \cot^p \frac{\theta_\ell}{2}. \quad (1)$$

Thus Λ_p is the p^{th} moment of $\cot \frac{\theta_\ell}{2}$ with respect to the distribution $|\langle\ell|t\rangle|^2$ over all $\ell \neq s$. Using these moments, we can define two quantities A and B as

$$A = \Lambda_1 - \cot \frac{\phi}{2}, \quad B = \sqrt{1 + \Lambda_2}. \quad (2)$$

It has been shown in [5] that a fast general algorithm is possible if and only if $A = O(\alpha B) \approx 0$ as typically $\alpha \ll 1$. Thus $\sum_{\ell \neq s} |\langle\ell|t\rangle|^2 \cot \frac{\theta_\ell}{2}$ must be almost equal to $\cot \frac{\phi}{2}$ for a fast quantum search. This is a very restrictive condition. In this paper, we present a modification of the general algorithm which does not require this kind of restrictive condition for its success. With this modification, the general algorithm becomes significantly flexible and works with a more general class of diffusion operators. Thus it allows for a successful quantum search in more general situations.

In next section, we present a brief review of the general algorithm. In Section III, we present the modification of the general algorithm. In Section IV, we discuss possible applications and conclude the paper.

II. GENERAL ALGORITHM

We briefly review the general algorithm [5]. It iterates the operator $\mathcal{S} = D_s I_t^\phi$ on $|s\rangle$. For simplicity, $|s\rangle$ is assumed to be a non-degenerate eigenstate of D_s with eigenvalue 1. The normalized eigenspectrum of D_s is given by $D_s|\ell\rangle = e^{i\theta_\ell}|\ell\rangle$. We have $\theta_{\ell=s} = 0$. Let other eigenvalues satisfy

$$|\theta_{\ell \neq s}| \geq \theta_{\min} > 0, \quad \theta_\ell \in [-\pi, \pi]. \quad (3)$$

*Electronic address: tulsi9@gmail.com

We need to find the eigenspectrum of \mathcal{S} to analyse its iteration on $|s\rangle$. The secular equation was found in [5] to be

$$\sum_{\ell} |\langle \ell | t \rangle|^2 \cot \frac{\lambda_k - \theta_{\ell}}{2} = \cot \frac{\phi}{2}. \quad (4)$$

Any eigenvalue $e^{i\lambda_k}$ of \mathcal{S} has to satisfy above equation.

Since $\cot x$ varies monotonically with x except for the jump from $-\infty$ to ∞ when x crosses zero, there is a unique solution λ_k between each pair of consecutive θ_{ℓ} 's. As $\theta_{\ell=s} = 0$, there can be at most two solutions λ_k in the interval $[-\theta_{\min}, \theta_{\min}]$. Let these two solutions be λ_{\pm} . We have $|\lambda_{\pm}| < \theta_{\min}$. The two eigenstates $|\lambda_{\pm}\rangle$ corresponding to these two eigenvalues $e^{i\lambda_{\pm}}$ are the only relevant eigenstates for our algorithm as the initial state $|s\rangle$ is almost completely spanned by these two eigenstates provided we assume $|\lambda_{\pm}| \ll \theta_{\min}$.

As shown in [5], the eigenphases λ_{\pm} are given by

$$\lambda_{\pm} = \pm \frac{2\alpha}{B} (\tan \eta)^{\pm 1}; \quad \cot 2\eta = \frac{A}{2\alpha B}. \quad (5)$$

where η is chosen to be within the interval $[0, \pi/2]$ and the quantities A and B are as defined in Eq. (2).

Eq. (20) of [5] gives us the target state $|t\rangle$ in terms of two relevant eigenstates $|\lambda_{\pm}\rangle$. We have

$$|t\rangle = \frac{|w\rangle}{B|\sin \frac{\phi}{2}|} + |\lambda_{\perp}\rangle, \quad |w\rangle = \sin \eta |\lambda_{+}\rangle + \cos \eta |\lambda_{-}\rangle, \quad (6)$$

where $|w\rangle$ is the normalized projection of $|t\rangle$ on the $|\lambda_{\pm}\rangle$ -subspace, and $|\lambda_{\perp}\rangle$ is a state orthogonal to this subspace.

Eq. (23) and (24) of [5] gives us the initial state $|s\rangle$ and the effect of iterating \mathcal{S} on $|s\rangle$ in terms of two relevant eigenstates $|\lambda_{\pm}\rangle$. We have

$$|s\rangle = e^{-i\phi/2} [e^{i\lambda_{+}/2} \cos \eta |\lambda_{+}\rangle - e^{i\lambda_{-}/2} \sin \eta |\lambda_{-}\rangle], \quad (7)$$

and

$$\mathcal{S}^q |s\rangle = e^{-i\phi/2} [e^{iq'\lambda_{+}} \cos \eta |\lambda_{+}\rangle - e^{iq'\lambda_{-}} \sin \eta |\lambda_{-}\rangle], \quad (8)$$

where $q' = q + \frac{1}{2}$.

The success probability of the algorithm is the probability of obtaining $|t\rangle$ upon measuring $\mathcal{S}^q |s\rangle$ which is $|\langle t | \mathcal{S}^q |s \rangle|^2$. Let this probability obtain its first maximum for $q = q_m$. Let us define a state $|u\rangle$ such that $|u\rangle = \mathcal{S}^{q_m} |s\rangle$. Then, by definition, the maximum success probability is

$$P_m = \beta^2, \quad \beta = |\langle t | u \rangle|. \quad (9)$$

Eq. (27) of [5] gives q_m and β as

$$q_m \approx \frac{\pi B \sin 2\eta}{4\alpha}, \quad \beta = \frac{\sin 2\eta}{B \sin \frac{\phi}{2}}. \quad (10)$$

The target state can be obtained with constant probability by $O(1/P_m)$ times repetitions of the general algorithm. Hence the total query complexity of the algorithm becomes

$$Q = \frac{q_m}{P_m} = \frac{q_m}{\beta^2} = \frac{\pi}{4\alpha} \frac{B^3 \sin^2 \frac{\phi}{2}}{\sin 2\eta}. \quad (11)$$

The minimum required number of queries by any quantum algorithm is $O(1/\alpha)$ and hence the general algorithm becomes inferior to the optimal algorithm if and only if $\sin 2\eta \ll 1$ which is true if $\cot 2\eta \gg 1$. By definition, this is true when $A \gg 2\alpha B$. Thus $A = O(\alpha B)$ is a necessary condition for the success of algorithm and as typically $\alpha \ll 1$, A must be close to zero. This is a very restrictive condition. In next section, we introduce a modification of the general algorithm which helps in getting rid off this condition.

III. MODIFIED GENERAL ALGORITHM

To get the basic idea behind modification, we note that $O(1/P_m)$ times repetitions of the general algorithm to boost the success probability to a constant value is basically a classical and inefficient process. In quantum setting, a far efficient method is available in the form of quantum amplitude amplification (hereafter referred to as QAA). In QAA, the $|u\rangle$ state is evolved to the target state $|t\rangle$ by $O(1/\beta)$ iterations of the QAA operator $I_t I_u$ on $|u\rangle$. By definition of the $|u\rangle$ state, we have

$$I_u = \mathcal{S}^{q_m} I_s \mathcal{S}^{-q_m}. \quad (12)$$

Thus implementation of I_u requires implementation of I_s . The question is that though I_t can be implemented easily, the same is not true for I_s and the entire motivation behind the construction of the general algorithm started with the hypothesis that we have only the operator D_s available and not I_s . This is what prevents us to use QAA to get the target state $|t\rangle$. We point out that I_s is not easily implementable in cases of physical interest [6–12]

To understand the modification of the general algorithm, we closely examine the possibility of implementing I_s . The $|s\rangle$ state is an eigenstate of the D_s operator with a known eigenvalue 1. Thus the phase estimation algorithm [13] (hereafter referred to as PEA) can be used to approximate I_s , the selective phase inversion of the $|s\rangle$ state, using multiple applications of the operator D_s .

In a recent paper (see Section III of [14]), we have presented a detailed algorithm for the approximate implementation of the selective phase inversion of the unknown eigenstates. There, the algorithm is presented to implement the operator $I_{\lambda_{\pm}}$ which is the selective phase inversion of the $|\lambda_{\pm}\rangle$ subspace of the operator \mathcal{S} . Note that there we have considered only a special case of the operator $\mathcal{S} = D_s I_t^{\phi}$ when ϕ is π and D_s is such that Λ_1 is zero. We have shown there that due to the assumption $|\lambda_{\pm}| \ll \theta_{\min}$, the operator $I_{\lambda_{\pm}}$ can be approximated with an error of ϵ using $O(\ln \epsilon^{-1}/\theta_{\min})$ applications of \mathcal{S} .

This is straightforward to extend the same ideas for approximate implementation of I_s as by definition, all eigenstates of D_s orthogonal to $|s\rangle$ have eigenphases greater than θ_{\min} and $|s\rangle$ is the only eigenstate satisfying $\theta_s = 0 \ll \theta_{\min}$. Thus I_s can be implemented with an error of ϵ using $O(\ln \epsilon^{-1}/\theta_{\min})$ applications of D_s .

In the general algorithm, the application of I_t as well as D_s takes unit time step. Thus the operator \mathcal{S} takes two time steps and Eq. (12) implies that $T[I_u]$ is $2q_m + T[I_s]$ where $T[X]$ denotes the time steps needed to implement the operator X . The discussion of the previous paragraph implies that

$$T[I_t I_u] = 2q_m + 1 + T[I_s] = O\left(q_m + \frac{\ln \epsilon^{-1}}{\theta_{\min}}\right). \quad (13)$$

Here ϵ is the desired error in implementation of I_s . For QAA, we need $O(1/\beta)$ applications of the operator $I_t I_u$ and hence same number of the approximate implementations of I_s . Thus the desired error in each approximate implementation of I_s is $O(\beta)$. The total time complexity of the algorithm is then

$$\frac{1}{\beta} O\left(q_m + \frac{\ln \beta^{-1}}{\theta_{\min}}\right). \quad (14)$$

Let us assume for a moment that

$$\frac{\ln \beta^{-1}}{\theta_{\min}} \not\gg q_m. \quad (15)$$

Then the second term in Eq. (14) can be ignored and the total time complexity of the algorithm becomes

$$O\left(\frac{q_m}{\beta}\right) = \frac{\pi B^2}{4\alpha} \sin \frac{\phi}{2}, \quad (16)$$

where we have used Eq. (10). Thus as desired, the time complexity is completely independent of η and A . As typically B and ϕ are $\Omega(1)$, the time complexity is close to the optimal performance of $O(1/\alpha)$.

The only condition to be satisfied by the algorithm is the assumption (15). Ignoring the logarithmic factor and using Eq. (10), the assumption becomes

$$\theta_{\min} \not\ll \frac{1}{q_m} = \frac{4\alpha}{\pi B} \frac{1}{\sin 2\eta} \approx \frac{4\alpha}{\pi B} \frac{A}{2\alpha B} = \frac{2A}{\pi B^2}, \quad (17)$$

where we have used Eq. (5) and the fact that $1/\sin 2\eta \approx \cot 2\eta$ whenever $\sin 2\eta \ll 1$. Note that if $\sin 2\eta \not\ll 1$ then there is no need to modify the general algorithm as the original general algorithm is also fast enough. The above condition can be rewritten as

$$A \not\gg 1.57 B^2 \theta_{\min}. \quad (18)$$

We compare it with the condition $A \not\gg 2\alpha B$ required for the success of the original general algorithm. As typically B is $\Theta(1)$ and $\theta_{\min} \gg \alpha$, the condition for the modified general algorithm is significantly relaxed compared to that for the original general algorithm.

IV. DISCUSSION AND CONCLUSION

We have shown that a modification of the general algorithm allows us to get a successful quantum search algorithm using a more general class of diffusion operators. The modification crucially depends upon the phase estimation algorithm and hence the quantum fourier transform.

A very important application of this modification is in tackling errors in diffusion operators. The original condition $A \not\gg 2\alpha B$ is a very restrictive condition as typically α is a very small quantity. Hence even minor deviations in the diffusion operator can cause failure of the original general algorithm. But the modified general algorithm is robust to such kind of small errors as this allows A to be as large as $O(\theta_{\min} B^2)$. This is a big relief as for typical diffusion operators, the quantity θ_{\min} is much bigger than α .

We hope that this modification will help us in designing fast quantum search algorithms under more general situations.

-
- [1] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
 - [2] L.K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
 - [3] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, Contemporary Mathematics (American Mathematical Society, Providence), **305**, 53 (2002) [arXiv.org:quant-ph/0005055].
 - [4] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Computing **26**, 1510 (1997) [arXiv.org:quant-ph/9701001].
 - [5] A. Tuli, Phys. Rev. A **86**, 042331 (2012).
 - [6] A. Ambainis, J. Kempe, and A. Rivosh, Proc. 16th ACM-SIAM SODA, p. 1099 (2005) [arXiv.org:quant-ph/0402107].
 - [7] A. Tuli, Phys. Rev. A **78**, 012310 (2008).
 - [8] A. Tuli, Phys. Rev. A **91**, 052307 (2015).
 - [9] A. Tuli, Phys. Rev. A **91**, 052322 (2015).
 - [10] G. Kato, Phys. Rev. A **72**, 032319 (2005).
 - [11] N. Shenvi, J. Kempe, and K. B. Whaley, Phys. Rev. A **67**, 052307 (2003).
 - [12] A. Ambainis, SIAM J. Computing, **37**, 210 (2007) [arXiv.org:quant-ph/0311001].
 - [13] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, England, 2000).
 - [14] A. Tuli, Phys. Rev. A **92**, 022353 (2015).